CLAIMS

1. An authentication method, wherein the method comprises:

when user equipment UE moves from a source trusted non-3rd generation partnership project 3GPP access point TNAP to a target TNAP, generating, by a trusted non-3GPP gateway function TNGF, an intermediate key based on a stored root key corresponding to the UE;

generating, by the TNGF, a target key for the target TNAP by using the intermediate key; and

sending, by the TNGF, the target key to the target TNAP, wherein the target key is used to protect communication security between the UE and the target TNAP.

2. The method according to claim 1, wherein generating, by the TNGF, the intermediate key based on the stored root key corresponding to the UE comprises:

generating, by the TNGF, the intermediate key based on a first usage type distinguisher and the root key, wherein the first usage type distinguisher is used to identify the generated intermediate key.

3. The method according to claim 1, wherein generating, by the TNGF, the intermediate key based on the stored root key corresponding to the UE comprises:

generating, by the TNGF, the intermediate key based on 0x03 and the root key.

4. The method according to any one of claims 1 to 3, wherein before generating, by the TNGF, the target key for the target TNAP by using the intermediate key, the method comprises:

sending, by the TNGF, an authentication request message to the UE through the target TNAP, wherein the authentication request message comprises a first verification parameter and a first freshness parameter, and the first verification parameter is generated by the TNGF based on the intermediate key and the first freshness parameter;

receiving, by the TNGF, an authentication response message from the UE, wherein the authentication response message comprises a second verification parameter and a second freshness parameter; and

obtaining, by the TNGF, a third verification parameter based on the intermediate key and the second freshness parameter; and

generating, by the TNGF, the target key for the target TNAP by using the intermediate key comprises:

when the third verification parameter matches the second verification parameter, generating, by the TNGF, the target key for the target TNAP by using the intermediate key.

5. The method according to any one of claims 1 to 3, wherein before generating, by the TNGF, the target key for the target TNAP by using the intermediate key, the method comprises:

sending, by the TNGF, an authentication request message to the UE through the target TNAP,

wherein the authentication request message comprises a first verification parameter and a first freshness parameter, and the first verification parameter is generated by the TNGF based on the root key and the first freshness parameter;

receiving, by the TNGF, an authentication response message from the UE, wherein the authentication response message comprises a second verification parameter and a second freshness parameter; and

obtaining, by the TNGF, a third verification parameter based on the root key and the second freshness parameter; and

generating, by the TNGF, the target key for the target TNAP by using the intermediate key comprises:

when the third verification parameter matches the second verification parameter, generating, by the TNGF, the target key for the target TNAP by using the intermediate key.

6. The method according to any one of claims 1 to 3, wherein after generating, by the TNGF, the target key for the target TNAP by using the intermediate key, and before sending, by the TNGF, the target key to the target TNAP, the method further comprises:

sending, by the TNGF, an authentication request message to the UE through the target TNAP, wherein the authentication request message comprises a first verification parameter and a first freshness parameter, and the first verification parameter is generated by the TNGF based on the intermediate key and the first freshness parameter;

receiving, by the TNGF, an authentication response message from the UE, wherein the authentication response message comprises a second verification parameter and a second freshness parameter; and

obtaining, by the TNGF, a third verification parameter based on the intermediate key and the second freshness parameter; and

sending, by the TNGF, the target key to the target TNAP comprises:

when the third verification parameter matches the second verification parameter, sending, by the TNGF, the target key to the target TNAP.

7. The method according to any one of claims 1 to 3, wherein after generating, by the TNGF, the target key for the target TNAP by using the intermediate key, and before sending, by the TNGF, the target key to the target TNAP, the method further comprises:

sending, by the TNGF, an authentication request message to the UE through the target TNAP, wherein the authentication request message comprises a first verification parameter and a first freshness parameter, and the first verification parameter is generated by the TNGF based on the root key and the first freshness parameter;

receiving, by the TNGF, an authentication response message from the UE, wherein the

authentication response message comprises a second verification parameter and a second freshness parameter; and

obtaining, by the TNGF, a third verification parameter based on the root key and the second freshness parameter; and

sending, by the TNGF, the target key to the target TNAP comprises:

when the third verification parameter matches the second verification parameter, sending, by the TNGF, the target key to the target TNAP.

8. The method according to claim any one of claims 1 to 3, wherein before generating, by the TNGF, the target key for the target TNAP by using the intermediate key, the method further comprises:

sending, by the TNGF, an authentication request message #1 to the UE through the target TNAP, wherein the authentication request message #1 comprises an identifier of the UE;

receiving, by the TNGF, an authentication response message #1 from the UE, wherein the authentication response message #1 comprises a second verification parameter and a second freshness parameter; and

obtaining, by the TNGF, a third verification parameter based on the intermediate key and the second freshness parameter;

generating, by the TNGF, the target key for the target TNAP by using the intermediate key comprises:

when the third verification parameter matches the second verification parameter, generating, by the TNGF, the target key for the target TNAP by using the intermediate key; and

after sending, by the TNGF, the target key to the target TNAP, the method further comprises:

sending, by the TNGF, an authentication request message #2 to the UE through the target TNAP, wherein the authentication request message #2 comprises a first verification parameter and a first freshness parameter, and the first verification parameter is generated by the TNGF based on the intermediate key and the first freshness parameter; and

receiving, by the TNGF, an authentication response message #2 from the UE through the target TNAP, wherein the authentication response message #2 indicates the TNGF to send an authentication success message.

9. The method according to any one of claims 1 to 3, wherein before generating, by the TNGF, the target key for the target TNAP by using the intermediate key, the method further comprises:

sending, by the TNGF, an authentication request message #1 to the UE, wherein the authentication request message #1 comprises an identifier of the UE;

receiving, by the TNGF, an authentication response message #1 from the UE, wherein the authentication response message #1 comprises a second verification parameter and a second

freshness parameter; and

obtaining, by the TNGF, a third verification parameter based on the root key and the second freshness parameter;

generating, by the TNGF, the target key for the target TNAP by using the intermediate key comprises:

when the third verification parameter matches the second verification parameter, generating, by the TNGF, the target key for the target TNAP by using the intermediate key; and

after sending, by the TNGF, the target key to the target TNAP, the method further comprises:

sending, by the TNGF, an authentication request message #2 to the UE through the target TNAP, wherein the authentication request message #2 comprises a first verification parameter and a first freshness parameter, and the first verification parameter is generated by the TNGF based on the root key and the first freshness parameter; and

receiving, by the TNGF, an authentication response message #2 from the UE through the target TNAP, wherein the authentication response message #2 indicates the TNGF to send an authentication success message.

10. The method according to any one of claims 1 to 9, wherein generating, by the TNGF, the target key for the target TNAP by using the intermediate key comprises:

generating, by the TNGF, the target key based on a second usage type distinguisher and the intermediate key, wherein the second usage type distinguisher is used to generate the target key.

11. The method according to any one of claims 1 to 10, wherein before generating, by the TNGF, the intermediate key based on the stored root key corresponding to the UE, the method further comprises:

receiving, by the TNGF, a first request message from the target TNAP; and

determining, by the TNGF in response to the first request message, that an authentication procedure between the TNGF and the UE needs to be performed.

12. The method according to claim 11, wherein the TNGF determines, based on the identifier of the UE, that the UE moves from the source TNAP to the target TNAP.

13. The method according to any one of claims 1 to 12, wherein before generating, by the TNGF, the intermediate key based on the stored root key corresponding to the UE, the method further comprises:

determining, by the TNGF, the root key based on the identifier of the UE.

14. An authentication method, wherein the method is applied to a scenario in which a communication apparatus moves from a source trusted non-3rd generation partnership project 3GPP access point TNAP to a target TNAP, and comprises:

generating, by the communication apparatus, an intermediate key based on a root key between

the communication apparatus and a trusted non-3GPP gateway function TNGF, wherein the TNGF is a management network element of the source TNAP and the target TNAP; and

generating, by the communication apparatus, a target key for the target TNAP by using the intermediate key, wherein the target key is used to protect communication security between the communication apparatus and the target TNAP.

15. The method according to claim 14, wherein generating, by the communication apparatus, the intermediate key based on the root key between the communication apparatus and the TNGF comprises:

generating, by the communication apparatus, the intermediate key based on a first usage type distinguisher and the root key, wherein the first usage type distinguisher is used to identify the generated intermediate key.

16. The method according to claim 14, wherein generating, by the communication apparatus, the intermediate key based on the root key between the communication apparatus and the TNGF comprises:

generating, by the communication apparatus, the intermediate key based on 0x03 and the root key.

17. The method according to any one of claims 14 to 16, wherein before generating, by the communication apparatus, the intermediate key based on the root key between the communication apparatus and the TNGF, the method comprises:

receiving, by the communication apparatus, an authentication request message from the TNGF through the target TNAP, wherein the authentication request message comprises a first verification parameter and a first freshness parameter, and the first verification parameter is generated by the TNGF based on the intermediate key and the first freshness parameter;

obtaining, by the communication apparatus, a fourth verification parameter by using the intermediate key and the first freshness parameter; and

when the fourth verification parameter matches the first verification parameter, sending, by the communication apparatus, an authentication response message to the TNGF, wherein the authentication response message comprises an identifier of the communication apparatus, a second verification parameter, and a second freshness parameter.

18. The method according to any one of claims 14 to 16, wherein before generating, by the communication apparatus, the intermediate key based on the root key between the communication apparatus and the TNGF, the method comprises:

receiving, by the communication apparatus, an authentication request message from the TNGF through the target TNAP, wherein the authentication request message comprises a first verification parameter and a first freshness parameter, and the first verification parameter is

generated by the TNGF based on the root key and the first freshness parameter;

obtaining, by the communication apparatus, a fourth verification parameter by using the root key and the first freshness parameter; and

when the fourth verification parameter matches the first verification parameter, sending, by the communication apparatus, an authentication response message to the TNGF, wherein the authentication response message comprises a second verification parameter and a second freshness parameter.

19. The method according to any one of claims 14 to 16, wherein before generating, by the communication apparatus, the intermediate key based on the root key between the communication apparatus and the TNGF, the method comprises:

receiving, by the communication apparatus, an authentication request message from the TNGF through the target TNAP, wherein the authentication request message comprises a first verification parameter and a first freshness parameter, and the first verification parameter is generated by the TNGF based on the root key and the first freshness parameter; and

obtaining, by the communication apparatus, a fourth verification parameter by using the intermediate key and the first freshness parameter;

generating, by the communication apparatus, the intermediate key based on the root key between the communication apparatus and the TNGF comprises: when the fourth verification parameter matches the first verification parameter, generating, by the communication apparatus, the intermediate key based on the root key between the communication apparatus and the TNGF; and

after generating, by the communication apparatus, the target key for the target TNAP by using the intermediate key, the method further comprises:

sending, by the communication apparatus, an authentication response message to the TNGF, wherein the authentication response message comprises an identifier of the communication apparatus, a second verification parameter, and a second freshness parameter.

20. The method according to any one of claims 14 to 16, wherein before generating, by the communication apparatus, the intermediate key based on the root key between the communication apparatus and the TNGF, the method comprises:

receiving, by the communication apparatus, an authentication request message from the TNGF through the target TNAP, wherein the authentication request message comprises a first verification parameter and a first freshness parameter, and the first verification parameter is generated by the TNGF based on the root key and the first freshness parameter; and

obtaining, by the communication apparatus, a fourth verification parameter by using the root key and the first freshness parameter;

generating, by the communication apparatus, the intermediate key based on the root key between the communication apparatus and the TNGF comprises: when the fourth verification parameter matches the first verification parameter, generating, by the communication apparatus, the intermediate key based on the root key between the communication apparatus and the TNGF; and

after generating, by the communication apparatus, the target key for the target TNAP by using the intermediate key, the method further comprises:

sending, by the communication apparatus, an authentication response message to the TNGF, wherein the authentication response message comprises an identifier of the communication apparatus, a second verification parameter, and a second freshness parameter.

21. The method according to any one of claims 14 to 20, wherein generating, by the communication apparatus, the target key for the target TNAP by using the intermediate key comprises:

generating, by the communication apparatus, the target key based on a second usage type distinguisher and the intermediate key, wherein the second usage type distinguisher is used to identify the generated target key.

22. The method according to claim 21, wherein before generating, by the communication apparatus, the intermediate key based on the root key between the communication apparatus and the TNGF, the method further comprises:

sending, by the communication apparatus, a first request message to the target TNAP.

23. The method according to claim 22, wherein the first request message comprises the identifier of the communication apparatus.

24. The method according to any one of claims 14 to 23, wherein before generating, by the communication apparatus, the intermediate key based on the root key between the communication apparatus and the TNGF, the method further comprises:

determining, by the communication apparatus, the root key based on an identifier of the TNGF.

25. A communication apparatus, wherein the communication apparatus comprises a module configured to perform the authentication method as the TNGF according to any one of claims 1 to 13.

26. A communication apparatus, wherein the communication apparatus comprises a module configured to perform the authentication method according to any one of claims 14 to 24.

27. A communication apparatus, wherein the communication apparatus comprises a processor, wherein

the processor is configured to perform the authentication method as the TNGF according to any one of claims 1 to 13; or

the processor is configured to perform the authentication method as the TNGF according to any one of claims 14 to 24.

28. A computer-readable storage medium, wherein the computer-readable storage medium comprises a computer program or instructions, and when the computer program or the instructions are run on a computer, the computer is enabled to perform the authentication method according to any one of claims 1 to 24.

29. A computer program product, wherein the computer program product comprises a computer program or instructions, and when the computer program or the instructions are run on a computer, the computer is enabled to perform the authentication method according to any one of claims 1 to 24.